

REMARKS

Claims 39, 41-45, 50-56, 58-59, and 70-155 are pending in the present application. By this Amendment, new claims 70-155 have been added.

The specification has been amended to include information on the related family applications, as requested by the Examiner. No new matter is added.

The claims have been amended to further clarify the invention and to improve form according to U.S. patent practice. New claims 70-155 recite various distinguishing features of the invention in a varying scope. The amended claims and the new claims are fully supported by the original disclosure, e.g., Figs. 1-3 and 5 and the corresponding description in the specification; column 3, line 59 – column 4, line 8 of the patent (page 11 of the specification); column 4, line 66 – column 5, line 11 of the patent (page 12 of the specification); column 6, lines 16-20 and 41-45 of the patent (page 14 of the specification). Thus, no new matter is added by the present Amendment.

35 U.S.C. §112, Second Paragraph, Rejection

Claim 39 has been rejected under 35 U.S.C. §112, second paragraph because the Examiner alleges that certain terms lack antecedent basis. Without acquiescing to this rejection, but to advance prosecution, claim 39 has been amended to further clarify the invention, in full compliance with 35 U.S.C. §112, second paragraph. Thus, reconsideration and withdrawal of this rejection are respectfully requested.

35 U.S.C. §101 Rejection

Claims 56 and 58-59 have been rejected under 35 U.S.C. §101 because the Examiner alleges that claim 56 merely recites nonfunctional descriptive material. This rejection is respectfully traversed.

Claim 56 recites credible utility and practical application of, e.g., control data and identification provided in the data storage medium. For instance, claim 56 recites that the identification information is “for indicating that at least a portion of the data group has a data

structure for copy prevention” and that the control data is “used for one or more succeeding data units in a scrambler/descrambler”, all of which impart functionality and practical application to the data storage medium and the data stored therein. Thus, claim 56 recites statutory subject matter, and reconsideration and withdrawal of this rejection are respectfully requested.

35 U.S.C. §103 Rejection

Claims 39, 41-45, 50-56 and 58-89 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Subler et al. in view of Kanota et al. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed.

First, Applicant respectfully submits that the claimed invention has a wide range of applicability in various fields. The Examiner has recognized this and thus has applied the specific references to reject the claims. Thus, Applicant has reviewed the applied references, Subler et al. and Kanota et al., and respectfully submit the following arguments.

Independent claim 39 recites, *inter alia*, “transmitting one or more scrambled data units, identification information, and control data as part of a data group”, “the identification information for indicating that at least a portion of the data group has a data structure for copy prevention,” and “wherein the scrambling step scrambles the digital data based on the control data such that the control data controls a parameter of the scrambling operation, the control data being used for one or more succeeding data units in the scrambling step.” Other independent claims recite similar features in a varying scope, e.g., descrambling based on the control data. All these features are neither taught nor suggested by the applied art.

Subler et al. is directed to ordering items and software through a computer. As shown in Fig. 20, Subler et al. displays an order information window 426 with customer information so that a customer can place a desired order; see, e.g., column 13, line 64 – column 14, line 3 of Subler et al. Once an order has been placed, the customer receives *separately* a decryption key, e.g., via a FAX or phone conversation with a clerk; see, e.g., column 14, lines 29-35 of Subler et al. Once the customer has the decryption key, the customer can enter the decryption key in the Unlock Order window 450 as shown in Fig. 21 to unlock the ordered item page, and can click on

the Install button 456 to download and install the ordered item (e.g., software); see, e.g., column 14, lines 40-55 of Subler et al.

The Examiner seems to equate the locking/unlocking operation of Subler et al. to Applicant's scrambling/descrambling. However, Subler et al. nowhere indicates that Subler's customer information (which the Examiner equates to Applicant's identification information) is "for indicating that at least a portion of the data group has a data structure for copy prevention" as recited in the independent claims.

Further, Subler et al. nowhere teaches or suggests transmitting the scrambled data along with control data and identification data, as part of a data group, where the control data is used for one or more succeeding data units in the scrambling or descrambling step, as recited in the independent claims. In Subler et al., the order page (which the Examiner equates as scrambled data) is transmitted to a user's computer and displayed there. However, Subler et al. fails to disclose that control data used in the scrambling or descrambling step, is also transmitted together with the scrambled data and the control data, as a data group, as in Applicant's claimed invention.

Moreover, in Applicant's claimed invention, the control data is used for one or more *succeeding* data units in the scrambling or descrambling step. Subler et al. is silent as to this claimed feature.

In the Office Action, the Examiner further relied on Kanota et al. to overcome the deficiencies of Subler et al. However, the above-noted deficiencies of Subler et al. are not corrected by Kanota et al.

Kanota et al. as shown in Fig. 1A transmits audio and video signals from the reproducing section 31 to the recording section 32 of Fig. 1B. However, the audio and video signals being transmitted are not scrambled signals. Thus, in Kanota et al., there is no transmitting the scrambled data, identification and control data as a data group, as required by the independent claims.

Further, in the recording section 32 as shown in Fig. 1B, Kanota et al. scrambles the received video signals before they are recorded. However, Kanota et al. is silent as to the

specifics of the scrambling operation, and thus fails to teach “the control data being used for one or more succeeding data units in the scrambling step” as recited in claim 39.

Moreover, Kanota’s scrambling occurs only when the ID (detected by the ID detection circuit 20) indicates that no copying is allowed, and no key is recorded with the scrambled data or known to a user. Once the scrambling occurs and the scrambled signals are recorded on the tape 27, Kanota’s pictures/video signals cannot be properly reproduced and thus copying is prevented. Thus, in Kanota et al., there is no descrambling of the scrambled data, and much less, there is no descrambling of the scrambled data based on the control data where the control data is used for one or more succeeding data units in the descrambling step, as recited in some of the independent claims.

Accordingly, independent claims 39, 45, 51 and 56 and their dependent claims (due to the dependency) are patentable over the applied art, and reconsideration and withdrawal of the rejection are respectfully requested.

New Claims

New claims 70-155 also recite distinguishing features of the invention in a varying scope. Thus, these claims are also believed to be allowable over the prior art of record.

CONCLUSION

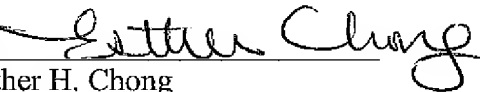
For the foregoing reasons and in view of the above clarifying amendments, the Examiner is respectfully requested to reconsider and withdraw all of the objections and rejections of record, and an early issuance of a Notice of Allowance is respectfully requested.

Should there be any matters which need to be resolved in the present application, the Examiner is respectfully requested to contact Esther H. Chong (Registration No. 40,953) at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37.C.F.R. §§1.16 or 1.14; particularly, extension of time fees.

Dated: June 6, 2008

Respectfully submitted,

By 

Esther H. Chong

Registration No.: 40,953

BIRCH, STEWART, KOLASCH & BIRCH, LLP

8110 Gatehouse Road

Suite 100 East

P.O. Box 747

Falls Church, Virginia 22040-0747

(703) 205-8000

Attorney for Applicant

Attachment: APPENDIX A – LIST OF ALL CLAIMS

APPENDIX A – LIST OF ALL CLAIMS

Original claims 1-38. (Canceled)

39. (Three Times Amended) A method for transmitting digital data, comprising:

scrambling digital data in data unit; and

transmitting ~~the one or more~~ scrambled ~~digital data units~~, identification information, and control data as part of a data group, the data group including a header and the header including the identification information and the control data, the identification information for indicating that at least a portion of the data group has a data structure for copy prevention,

wherein the scrambling step scrambles the digital data based on the control data such that the control data controls a parameter of the scrambling operation, the control data being used for one or more succeeding data units in the scrambling step.

40. (Canceled)

41. (Twice Amended) The method of claim 39, ~~wherein the transmitting step transmits the control data as part of the data group~~ further comprising:

combining the one or more scrambled data units and the header into the data group, before the transmitting step.

42. The method of claim 39, further comprising:

encrypting the control data prior to the transmitting step; and

wherein the transmitting step transmits the encrypted control data as part of the data group.

43. The method of claim 42, wherein the encrypting step encrypts the control data based on a key.

44. (Amended) The method of claim 39, wherein the data group further includes copy prevention information, the copy prevention information ~~includes~~including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and
wherein the copy prevention information is used for performing a copy prevention function in a receiving part.

45. (Three Times Amended) A method for recording digital data, comprising:
scrambling digital data in data unit; and
recording ~~the one or more~~ scrambled digital data units, identification information, and control data as part of a data group, the data group including a header and the header including the identification information and the control data, the identification information for indicating that at least a portion of the data group has a data structure for copy prevention,
wherein the scrambling step scrambles the digital data based on the control data such that the control data controls a parameter of the scrambling operation, the control data being used for one or more succeeding data units in the scrambling step.

46-49. (Canceled)

50. (Amended) The method of claim 45, wherein the data group further includes copy prevention information, the copy prevention information ~~includes~~including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and
wherein the copy prevention information is used for performing a copy prevention function in a reproducing/recording part.

51. (Amended) A method of processing ~~protected~~ digital data, comprising:

receiving a data group including identification information, control data and scrambled digital data, the data group ~~also having including~~ a header and the header including the identification information, the identification information for indicating that at least a portion of the data group has a data structure for copy prevention; and

descrambling the scrambled digital data based on the control data, the control data being used for one or more succeeding data units in the descrambling step.

52. (Amended) The method of claim 51, wherein

the receiving step further receives copy prevention information as part of the data group, and the method further comprises:including,

performing a copy prevention function based on the copy prevention information.

53. The method of claim 51, wherein

the receiving step receives encrypted control data as part of the data group; and the method further includingcomprises;

decrypting the encrypted control data prior to the descrambling step.

54. The method of claim 53, wherein the decrypting step decrypts the control data using a key.

55. (Amended) The method of claim ~~51~~52, wherein the copy prevention information includes one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and wherein the performing step performs the copy prevention function such that copying of digital data is not permitted if the copy prevention information indicates that copying of digital data is not permitted, and

wherein the descrambling step is performed only if the copy prevention information indicates that copying of digital data is permitted.

56. (Four Times Amended) A data storage medium, comprising:

a data ~~group~~-area including at least one data group, the data group comprising a header area and a digital data-area;

the header ~~area~~-including an identification information area and a control data-area;
~~the identification area including the~~ identification information for indicating that at least a portion of the data group has a data structure for copy prevention;

the control data area ~~including control data such that the control data controls for~~ controlling a parameter of a scrambling operation; and

the digital data ~~area~~-including digital data one or more data units scrambled based on the control data, the control data being used for one or more succeeding data units in a scrambler/descrambler.

57. (Canceled)

58. (Three Times Amended) The data storage medium of claim 56, wherein the control data ~~area~~ stores comprises encrypted control data encrypted by a key.

59. (Twice Amended) The data storage medium of claim 56, wherein the data group further includes copy prevention information ~~is provided in the control data area and~~, the copy prevention information includes ~~including~~ one of current generation information and allowable generation information, the current generation information indicating a number of times digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data.

60-69. (Canceled)

70. (New) The method of claim 39, wherein the data group includes at least two packets, at least first packet including one data unit and the header, and

wherein the scrambling step scrambles the data unit except for the header.

71. (New) The method of claim 39, wherein the scrambling step scrambles the digital data in such a manner that the digital data is protected.

72. (New) The method of claim 45, wherein the data group includes at least two packets, at least first packet including one data unit and the header, and

wherein the scrambling step scrambles the data unit except for the header.

73. (New) The method of claim 45, wherein the scrambling step scrambles the digital data in such a manner that the digital data is protected.

74. (New) The method of claim 51, wherein the data group includes at least two packets, at least first packet including one data unit and the header, and

wherein the descrambling step descrambles the data unit except for the header.

75. (New) The method of claim 74, further comprising:

extracting the header from the packet, and

wherein the descrambling step descrambles the data unit except for the header based on the control data.

76. (New) The method of claim 51, wherein the descrambling step descrambles the digital data in such a manner that the digital data is not protected.

77. (New) The data storage medium of claim 56, wherein the data group includes at least two packets, at least first packet including one data unit and the header.

78. (New) The data storage medium of claim 56, wherein the digital data is scrambled in such a manner that the digital data is protected.

79. (New) An apparatus for transmitting digital data, comprising:

a scrambler to scramble digital data in data unit; and

a controller operatively coupled to control the scrambler, and to control a transmission of the scrambled one or more data units, identification information and control data as part of a data group, the data group including a header, the header including the identification information and the control data, the identification information for indicating that at least a portion of the data group has a data structure for copy prevention,

wherein the scrambler is configured to scramble the digital data based on the control data such that the control data controls a parameter of the scrambling operation, according to a control of the controller, the control data being used for one or more succeeding data units in the scrambler.

80. (New) The apparatus of claim 79, further comprising:

a multiplexer to combine the one or more scrambled data units and the header into one data group before the transmission.

81. (New) The apparatus of claim 79, further comprising:

an encryption unit to encrypt the control data prior to the transmission, and

wherein the controller is configured to transmit the encrypted control data as part of the data group.

82. (New) The apparatus of claim 81, wherein the encryption unit is configured to encrypt the control data based on a key, according to a control of the controller.

83. (New) The apparatus of claim 79, wherein the header further includes copy prevention information, the copy prevention information including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and

wherein the copy prevention information is used for performing a copy prevention function in a receiving apparatus.

84. (New) The apparatus of claim 79, wherein the data group includes at least two packets, at least first packet including one data unit and the header, and

wherein the scrambler is configured to scramble the data unit except for the header.

85. (New) The apparatus of claim 79, wherein the scrambler is configured to scramble the digital data in such a manner that the digital data is protected.

86. (New) An apparatus for recording digital data, comprising:

a scrambler to scramble digital data in data unit; and

a controller operatively coupled to the scrambler, and to control a recording of one or more scrambled units, identification information, and control data as part of a data group, the data group including a header and the one or more scrambled data units, the header including the identification information and the control data, the identification information for indicating that at least a portion of the data group has a data structure for copy prevention,

wherein the scrambler is configured to scramble the digital data based on the control data such that the control data controls a parameter of the scrambling operation according to a control of the controller, the control data being used for one or more succeeding data units in the scrambler.

87. (New) The apparatus of claim 86, further comprising:

a multiplexer to combine the one or more scrambled data units and the header into one data group before the recording.

88. (New) The apparatus of claim 86, further comprising:

an encryption unit to encrypt the control data prior to the recording, and

wherein the controller is configured to record the encrypted control data as the data group.

89. (New) The apparatus of claim 88, wherein the encryption unit is configured to encrypt the control data based on a key, according to a control of the controller.

90. (New) The apparatus of claim 86, wherein the data group further includes copy prevention information, the copy prevention information including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and

wherein the copy prevention information is used for performing a copy prevention function in a reproducing/recording apparatus.

91. (New) The apparatus of claim 86, wherein the data group includes at least two packets, at least first packet including one data unit and the header, and

wherein the scrambler is configured to scramble the data unit except for the header.

92. (New) The apparatus of claim 86, wherein the scrambler is configured to scramble the digital data in such a manner that the digital data is protected.

93. (New) An apparatus for processing digital data, comprising:

a receiving part to receive a data group including identification information, control data and scrambled digital data, the data group comprising one or more scrambled data units and a header, the header including the identification information, the identification information for indicating that at least a portion of the data group has a data structure for copy prevention;

a descrambler to descramble the scrambled digital data based on the control data, the control data being used for one or more succeeding data units in the descrambler; and

a controller operatively coupled to the descrambler to control a descrambling operation.

94. (New) The apparatus of claim 93, wherein the data group further includes copy prevention information, the copy prevention information including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and

wherein the controller is configured to control a copy prevention function based on the copy prevention information such that copying of digital data is not permitted if the copy prevention information indicates that copying of digital data is not permitted.

95. (New) The apparatus of claim 94, wherein the controller is configured to control the descrambler such that the descrambling of the scrambled data unit by the descrambler is performed only if the copy prevention information indicates that copying of digital data is permitted.

96. (New) The apparatus of claim 93, wherein the received control data is an encrypted control data, and the apparatus further comprises:

a decryption unit to decrypt the encrypted control data using a key prior to the descrambling, according to a control of the controller.

97. (New) The apparatus of claim 93, wherein the data group includes at least two packets, at least first packet including one data unit and the header, and

wherein the descrambler is configured to descramble the data unit except for the header.

98. (New) The apparatus claim 93, further comprising:

an extraction unit to extract the header from a data block, and

wherein the descrambler is configured to descramble the data unit except for the header based on the control data, according to a control of the controller.

99. (New) The apparatus of claim 93, wherein the descrambler is configured to descramble the digital data in such a manner that the digital data is not protected.

100. (New) A method of transmitting digital data, comprising:

scrambling digital data in data unit; and

transmitting one or more scrambled data units and control data, the control data being used for controlling a parameter of a scrambling/descrambling operation and the same control data being used for one or more succeeding data units in the scrambling step.

101. (New) The method of claim 100, wherein the control data is used to initialize a scrambler for performing the scrambling operation, and

wherein the scrambling step includes initializing the scrambler based on the control data.

102. (New) The method of claim 100, wherein the digital data comprises a plurality of data blocks including a first data block, each data block including a header and one data unit, at least the header in the first data block including the control data, and

wherein the scrambling step scrambles each data unit except for the header in each data block.

103. (New) The method of claim 100, wherein the control data is changed or refreshed periodically, and

wherein the scrambling step scrambles one or more succeeding data units based on the changed or refreshed control data.

104. (New) The method of claim 100, further comprising:

multiplexing at least two scrambled data units and the control data into one data group before the transmitting step.

105. (New) The method of claim 104, wherein the data group includes at least two packets, at least first packet including one data unit and a header, the header including the control data, and
wherein the multiplexing step multiplex the at least two packets into one data group before the transmitting step.

106. (New) The method of claim 100, wherein the scrambling step scrambles the digital data in such a manner that the digital data is protected.

107. (New) The method of claim 104, wherein the data group further includes copy prevention information, the copy prevention information including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and

the copy prevention information being used for a copy prevention function in a receiving part.

108. (New) An apparatus for transmitting digital data, comprising:

a scrambler to scramble digital data in data unit; and

a controller operatively coupled to control the scrambler, and to control a transmission of one or more scrambled data units and control data, the control data being used for controlling a parameter of a scrambling/descrambling operation and the same control data being used for one or more succeeding data units in the scrambler.

109. (New) The apparatus of claim 108, wherein the control data is used to initialize a scrambler for performing the scrambling operation, and

wherein the controller is configured to initialize the scrambler based on the control data.

110. (New) The apparatus of claim 108, wherein the digital data comprises a plurality of data blocks including a first data block, each data block including one data unit and a header, at least the header in the first data block including the control data, and

wherein the scrambler is configured to scramble each data unit except for the header in each data block, according to a control of the controller.

111. (New) The apparatus of claim 108, wherein the control data is changed or refreshed periodically, and

wherein the controller is configured to control the scrambler to scramble one or more succeeding data units based on the changed or refreshed control data.

112. (New) The apparatus of claim 108, further comprising:

a multiplexer to multiplex at least two scrambled data units and a header into one data group before the transmission, the header including the control data.

113. (New) The apparatus of claim 112, wherein the data group includes at least two packets, at least first packet including one data unit and the header, and

wherein the multiplexer is configured to multiplex the at least two packets into one data group.

114. (New) The apparatus of claim 108, wherein the scrambler is configured to scramble the digital data in such a manner that the digital data is protected.

115. (New) The apparatus of claim 112, wherein the data group further includes copy prevention information, the copy prevention information including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and the copy prevention information being used for a copy prevention function in a receiving apparatus.

116. (New) A method of recording digital data, comprising:

scrambling digital data in data unit; and

recording one or more scrambled data units and control data in a data storage, the control data being used for controlling a parameter of a scrambling/descrambling operation and the same control data being used for one or more succeeding data units in the scrambling step.

117. (New) The method of claim 116, wherein the control data is used to initialize a scrambler for performing the scrambling operation, and

wherein the scrambling step includes initializing the scrambler based on the control data.

118. (New) The method of claim 116, wherein the digital data comprises a plurality of data blocks including a first data block, each data block including one data unit and a header, at least the header in the first data block including the control data, and

wherein the scrambling step scrambles each data unit except for the header in each data block.

119. (New) The method of claim 116, wherein the control data is changed or refresh periodically, and

wherein the scrambling step scrambles one or more succeeding data units based on the changed or refreshed control data.

120. (New) The method of claim 116, further comprising:

multiplexing at least two scrambled data units and a header into one data group before the recording step, the header including the control data.

121. (New) The method of claim 120, wherein the data group includes at least two packets, at least first packet including one data unit and the header, and

wherein the multiplexing step multiplexes the at least two packets into one data group.

122. (New) The method of claim 116, wherein the scrambling step scrambles the digital data in such a manner that the digital data is protected.

123. (New) The method of claim 120, wherein the data group further includes copy prevention information, the copy prevention information including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and

the copy prevention information being used for a copy prevention function in a reproducing /recording part.

124. (New) An apparatus for recording digital data, comprising:

a scrambler to scramble digital data in data unit;

a recording unit to record the scrambled digital data; and

a controller operatively coupled to control the scrambler and to control the recording unit to record one or more scrambled data units and control data in a data storage, the control data being used for controlling a parameter of a scrambling/descrambling operation and the same control data being used for one or more succeeding data units in the scrambler.

125. (New) The apparatus of claim 124, wherein the control data is used to initialize the scrambler for performing the scrambling operation, and

wherein the controller is configured to initialize the scrambler based on the control data.

126. (New) The apparatus of claim 124, wherein the digital data comprises a plurality of data blocks including a first data block, each data block including one data unit and a header, at least the header in the first data block including the control data, and

wherein the scrambler is configured to scramble each data unit except for the header in each data block.

127. (New) The apparatus of claim 124, wherein the control data is changed or refreshed periodically, and

wherein the controller is configured to control the scrambler to scramble one or more succeeding data units based on the changed or refreshed control data.

128. (New) The apparatus of claim 124, further comprising:

a multiplexer to multiplex at least two scrambled data units and a header into one data group before the recording, the header including the control data.

129. (New) The apparatus of claim 128, wherein the data group includes at least two packets, at least first packet including one data unit and the header, and

wherein the multiplexer is configured to multiplex the at least two packets into one data group.

130. (New) The apparatus of claim 124, wherein the scrambler is configured to scramble the digital data in such a manner that the digital data is protected.

131. (New) The apparatus of claim 128, wherein the data group further includes copy prevention information, the copy prevention information including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and the copy prevention information being used for a copy prevention function in a reproducing/recording apparatus.

132. (New) A method of processing digital data, comprising:

receiving one or more scrambled data units and a control data, the control data being used for controlling a parameter of a scrambling/descrambling operation and the same control data being used for one or more succeeding data units; and

descrambling the one or more scrambled data units and the one or more succeeding data units based on the same control data.

133. (New) The method of claim 132, wherein the control data is used to initialize a descrambler for performing the descrambling operation, and

wherein the descrambling step includes initializing the descrambler based on the control data.

134. (New) The method of claim 132, wherein the digital data comprises a plurality of data blocks including a first data block, each data block including one data unit and a header, at least the header in the first data block including the control data, and

wherein the descrambling step descrambles the data unit except for the header.

135. (New) The method of claim 132, wherein the control data is changed or refreshed periodically, and

wherein the descrambling step descrambles one or more succeeding data units based on the changed or refreshed control data.

136. (New) The method of claim 132, wherein at least two scrambled data units and a header including the control data comprise one data group, the header including the control data, and

Wherein the method further comprises:

demultiplexing the at least two scrambled data units and the header from one data group before the descrambling step.

137. (New) The method of claim 136, wherein the data group includes at least two packets, at least first packet including the header, and

wherein the demultiplexing step demultiplexes the at least two packets from one data group.

138. (New) The method of claim 132, wherein the descrambling step descrambles the digital data in such a manner that the digital data is not protected.

139. (New) The method of claim 132, wherein the receiving step further receives copy prevention information, the copy prevention information including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and

Wherein the method further comprises:

performing a copy prevention function such that copying of digital data is not permitted if the copy prevention information indicates that copying of digital data is not permitted.

140. (New) The method of claim 139, wherein the descrambling step is performed only if the copy prevention information indicates that copying of digital data is permitted.

141. (New) An apparatus for processing digital data, comprising:

a receiving part to receive a control data and one or more scrambled data units, the control data being used for controlling a parameter of a scrambling/descrambling operation and the same control data being used for one or more succeeding data units;

a descrambler to descramble the received one or more scrambled data units and one or more succeeding data units based on the same control data; and

a controller, operatively coupled to the descrambler, to control the descrambling operation by the descrambler.

142. (New) The apparatus of claim 141, wherein the control data is used to initialize the descrambler for performing the descrambling operation, and

wherein the controller is configured to initialize the descrambler based on the control data.

143. (New) The apparatus of claim 141, wherein the digital data comprises a plurality of data blocks including a first data block, each data block including one data unit and a header, at least the header in the first data block including the control data, and

wherein the descrambler is configured to descramble each data unit except for the header in each data block.

144. (New) The apparatus of claim 141, wherein the control data is changed or refreshed periodically, and

wherein the controller is configured to control the descrambler to descramble one or more succeeding data units based on the changed or refreshed control data.

145. (New) The apparatus of claim 141, wherein at least two scrambled data units and a header including the control data comprise one data group, the header including the control data, and

wherein the apparatus further comprises:

a demultiplexer to separate the at least two scrambled data units and the header from one data group before the descrambling.

146. (New) The apparatus of claim 145, wherein the data group includes at least two packets, at least first packet including one data unit and the header, and

wherein the demultiplexer is configured to demultiplex the at least two packets from one data group.

147. (New) The apparatus of claim 145, further comprising:

a detector to detect the header from the received data group and to detect the control data within the header.

148. (New) The apparatus of claim 145, wherein the data group further includes copy prevention information, the copy prevention information including one of current generation information and allowable generation information, the current generation information indicating a number of

times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and

wherein the controller is further configured to control a copy prevention function such that copying of digital data is not permitted if the copy prevention information indicates that copying of digital data is not permitted.

149. (New) The apparatus of claim 141, wherein the descrambling of scrambled digital data by the descrambler is performed only if the copy prevention information indicates that copying of digital data is permitted.

150. (New) A data storage medium comprising:

one or more scrambled data units and control data stored on the data storage medium, wherein the control data is used for controlling a parameter of a scrambling/descrambling operation and the same control data is used for one or more succeeding data units.

151. (New) The data storage medium of claim 150, wherein the control data is used to initialize a scrambler for performing the scrambling operation.

152. (New) The data storage medium of claim 150, wherein the data storage medium includes a plurality of data blocks including a first data block, each data block including one data unit and a header, at least the header in the first data block including the control data, and

wherein each data unit is scrambled while the header is not scrambled, in each data block.

153. (New) The data storage medium of claim 150, wherein the control data is changed or refreshed periodically, and

wherein one or more succeeding data units are scrambled based on the changed or refreshed control data.

154. (New) The data storage medium of claim 150, wherein at least two packets comprise one data group, at least first packet including one scrambled data unit and a header, the header including the control data.

155. (New) The data storage medium of claim 150, wherein one or more scrambled data units and control data comprise one data group, the data group further including copy prevention information, the copy prevention information including one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data, and the copy prevention information being used for a copy prevention function in a reproducing/reproducing/recording apparatus such a manner that copying of digital data is not permitted if the copy prevention information indicates that copying of digital data is not permitted.